



ABOVE BOARD

A quarterly newsletter published by
the Office of the Information and Privacy Commissioner

Volume 17, Issue 2

April 2025

Contact Information

Office of the Information
and Privacy Commissioner

Mailing Address:
P.O. Box 13004, Station A
St. John's, NL
A1B 3V8

Telephone:

709-729-6309

Fax:

709-729-6500

Toll Free in Newfoundland
and Labrador:

1-877-729-6309

Email:

commissioner@oipc.nl.ca

Website:

www.oipc.nl.ca

Follow us on social media!

LinkedIn:

[https://LinkedIn.com/com
pany/oipc-nl](https://LinkedIn.com/company/oipc-nl)

This Issue:

- OIPC Office has Moved
- Time Extensions
- New and Updated Forms, Guidelines, and Guidance
- Nova Scotia Access to Information Legislation Update
- The Value of Information Management in Access and Privacy
- ATIPPA, 2015 Privacy Breach Statistics January 1 – March 31, 2025

OIPC Office has Moved

OIPC has moved to a new office space! After a decade in the Sir Brian Dunfield Building, we have a new physical office space located in the Beothuck Building here in St. John's, NL. Please note that OIPC is currently closed to walk-in traffic due to renovations; we cannot accommodate in-person inquiries at this time.

Our New Physical Address is:

20 Crosbie Place
Beothuck Building
St. John's NL

Our Mailing Address, Telephone Numbers and Email Remain the Same

Mailing Address

P.O. Box 13004, Station A
St. John's, NL A1B 3V8

Telephone: 709-729-6309
Toll Free in Newfoundland and
Labrador: 1-877-729-6309

Email: commissioner@oipc.nl.ca

Time Extensions

Section 16 of the **Access to Information and Protection of Privacy Act, 2015** (ATIPPA, 2015) requires a public body to respond to an access to information request within 20 business days of its receipt. However, under section 23, a public body may apply to OIPC to extend this time. An application to extend the time for responding to a request must be made within 15 business days of receiving the request (or, in other words, at least five days before the response to the request is due).

Process

OIPC has a form for applying for an extension on our [website](#). Completed forms should be sent to commissioner@oipc.nl.ca. There is no need to send an extension application to anyone else in our Office. An application should contain as much detail as possible, in particular: the number of records located to date in the public body's search, any consultations required (whether with third parties, other public bodies in the province, or with other jurisdictions), and the public body's existing caseload of access requests. If details are missing or insufficient, an extension might not be approved, or only partially approved.

Our Office will respond to applications within three business days, as required by section 23(3). Applications received after 4:30 pm will be considered as received the next business day, which will affect the time for our response and may also affect whether the public body meets the deadline for applying for an extension.

If an extension is approved, section 23(6) requires a public body to notify the access to information applicant that an extension has been approved by the Commissioner, the reasons for the extension, and when a response can be expected. A de-identified copy of this notice should be sent to our Office at commissioner@oipc.nl.ca. It is not necessary to send the notice to anyone else.

Subsequent Extensions

Most often, a public body will seek an extension of between 10 and 20 business days and will complete the request in that additional time. However, more challenging requests may require a lengthier extension of time (roughly, any extension more than 40 business days). Public bodies should be aware that such lengthy extensions of time are unlikely to be approved in full, but we can accept multiple time extension applications for the same access request. Subsequent applications should identify progress made on completing the request since the last application.

A public body should identify the time needed in its initial application, even if full approval is unlikely. By approving partial extensions and monitoring progress, our Office can fulfill its oversight role while helping the public body manage its workload. For example, if a public body anticipates needing 60 additional business days, it should request 60 days, even if our Office only approves 40. In a subsequent application, the public body can request additional time with updates on progress, consultations, and the number of pages processed. This approach is more efficient than repeatedly requesting shorter extensions.

If a public body has applied for more time than was approved, and anticipates applying for a further extension of time, a best practice would be to note this in its notice to the applicant. Telling an applicant "with approval from the Information and Privacy Commissioner . . . the 20 business day time limit for responding to your request has been extended for an additional 20 days with a new

deadline of [date]; however, we expect to require a further extension of time in order to complete your request and will inform you of any updates” will help better manage expectations and the relationship with an applicant than providing them with multiple new deadlines that the public body does not expect to be able to meet.

As mentioned earlier, an application for a time extension must come at least five days before the response to the request is due. Public bodies should follow this five-day rule for subsequent extension applications as well. If our Office has approved a 20-business day extension (giving the public body a total of 40 days to respond to the request) and the public body requires further time, it should apply for a second time extension before day 35 has passed.

What Time Extensions Are Not Intended For

Public bodies should be mindful that a time extension under section 23 is intended to allow public bodies additional time to respond to particularly challenging requests (large volumes of records or requests that require consultations with other public bodies) or to manage unusual circumstances (a large number of requests received at one time or key personnel are unavailable). Public bodies should not rely on section 23 as a routine matter for its access requests. Rather, public bodies should assess whether additional personnel or other resources should be dedicated to managing the public body’s access request caseload if it finds itself regularly applying for time extensions.

Public bodies should also not expect to use a time extension to extend the 20 business days for responding to an access request solely to accommodate executive review of a response.

Key Takeaways for Time Extensions!

1. Public bodies have 20 business days to respond to an access request,
2. Section 23 allows time extension requests,
3. Extension applications **must** be emailed to commissioner@oipc.nl.ca,
4. De-identified notices to applicants **must** be emailed to commissioner@oipc.nl.ca,
5. OIPC can accept subsequent extension applications,
6. Subsequent extension applications **must** follow the five-day rule,
7. Estimate total time needed in your first request, if possible, and
8. Extensions should be for complex requests or special circumstances, not overused.

New and Updated Forms, Guidelines and Guidance

Our Office has updated its breach reporting form and guidelines to assist public bodies. We ask all coordinators to use the new form when reporting a privacy breach under ATIPPA, 2015.

To view the latest versions of the form and guidelines, please visit the links below:

- [Reporting a Privacy Breach Form](#).
- [How to Complete the Reporting a Privacy Breach Form](#).

[Reasonable Safeguards](#) - This new guidance is intended to assist custodians and public bodies understand their obligation to ensure reasonable safeguards are in place.

[Use of Video Surveillance](#) – This new guidance addresses public bodies and custodians that are using or are considering using video surveillance. Please note that the **OIPC Guidelines for Video Surveillance by Public Bodies in Newfoundland and Labrador**, a more detailed document on video surveillance use by public bodies, has been moved to the [Archive](#) page on our website. The guidance piece **OIPC Guidelines for the Use of Video Surveillance Systems in Schools** has been removed from our website as it references the former **Access to Information and Protection of Privacy Act**; however, interested individuals can obtain a copy by contacting our Office.

[PIAs: What is Personal Information](#) – This new guidance is the first of a number of resources intended to assist public bodies working on privacy impact assessments (PIAs). Watch the PIA section on our guidance page for more resources as they become available!

If you have any questions or feedback about our forms, guidelines, or guidance, including suggestions on topics for guidance resources, please let us know!

Nova Scotia Access to Information Legislation Update

On February 18, 2025, [Bill 1: An Act Respecting Government Organization and Administration](#) was introduced in Nova Scotia's Legislature; it received royal assent on March 26, 2025. Part IV of this Bill includes amendments to the **Freedom of Information and Protection of Privacy Act** (FOIPOP).

Some highlights of the amendments include:

- Requiring specific details from requestors. Requests must either specify the record requested or, where this is unknown, provide sufficient particulars as to time, place and event to enable a person familiar with the topic or issue to identify the requested record. Section 6(3) of the Bill further clarifies "...where a request is made for records in the form of electronic mail written by a person or between persons, the request must specify the topic or issue of the requested records with reasonable efforts to list particulars, such as time, place, event and subject."
- Ability for the head of the public body to disregard requests in certain circumstances, including if sufficient particulars are not provided.

While the Bill contains additional review considerations for OIPC NS, it does not appear that its government has contemplated additional resources to address these new responsibilities, which could lead to missed deadlines.

It should be noted that the Bill, as originally introduced, included some other provisions that could have had a negative impact on access rights. However, commentary and feedback received by government from the public resulted in positive changes to the Bill, which emphasizes the importance of public debate on such matters.

Anyone interested in learning more can review the Bill on the NS Legislature site ([Nova Scotia Legislature - Bill 1 – An Act Respecting Government Organization and Administration](#)).

The Value of Information Management in Access and Privacy

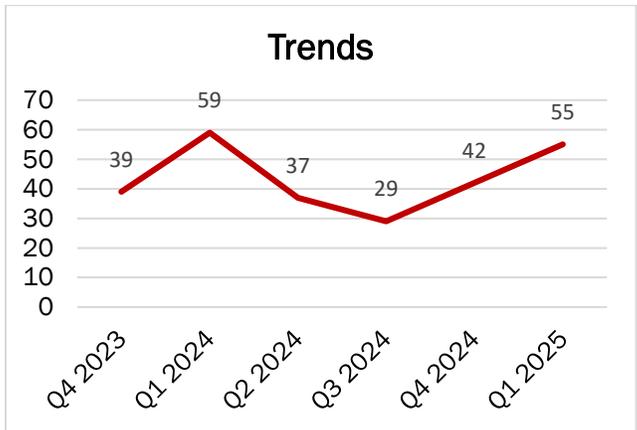
Information Management (IM) may be defined as the processes and technology that controls the storage, structure, processing, access, and usage of the information required for organizational and business intelligence. IM plays a critical role in access to information, privacy, and security. If you do not know what information you have, where it is stored, and who has access to it, how can you be in compliance with legislation like ATIPPA, 2015 or the **Management of Information Act**? IM professionals organize and manage all activities involved in the information life cycle, automating processes, reducing operating costs, and improving efficiencies.

The College of the North Atlantic (CNA) offers an information management post-diploma program for individuals interested in becoming an IM professional. This three-semester online program equips graduates with the skills to implement IM best practices in training and consultation, ensuring organizational compliance with regulatory standards, including security, legal, and privacy requirements. Further information about the program is available on CNA’s website at [Information Management-College of the North Atlantic](#).

ATIPPA, 2015 Privacy Breach Statistics January 1 – March 31, 2025

During the first quarter of 2025 (January 1 – March 31, 2025), OIPC accepted 55 privacy breach reports from 20 public bodies under ATIPPA, 2015. This is an increase from the 42 breaches reported during the previous quarter. There were two intentional breaches reported during this quarter. One involved the disclosure of unnecessary personal information in correspondence on another topic and the other involved access to file information by cleaning staff. The numbers indicate that email breaches continue to make up a very significant portion of the overall privacy breaches reported.

Summary by Public Body			
Central Newfoundland Waste Management	Newfoundland	Waste	1
City of St. John's			1
College of the North Atlantic			1
Department of Children, Seniors and Social Development			4
Department of Digital Government and Service NL			7
Department of Education			11



Department of Fisheries, Forestry and Agriculture	1
Department of Immigration, Population Growth and Skills	1
Department of Justice and Public Safety	2
Department of Labrador Affairs	1
Labour Relations Board	2
Memorial University	7
Newfoundland and Labrador Housing Corporation	5
NL Health Services	2
NL Hydro	2
Public Service Commission	2
Royal Newfoundland Constabulary	1
The Rooms	1
Town of Port au Port East	1
Workplace NL	2

